ABSTRACT

A method for mutual authentication of components in a network using a challenge-response method, including the steps of requesting at least one data pair including a first random number and a first response from an authentication center, passing the first random number to a terminal which uses an internally stored key and the first random number to calculate the first response, sending the calculated first response to the network, sending a second random number from the terminal to the network, and responding to the second random number with a second response calculated in the authentication center. The first response sent from the terminal to the network is also used as the second random number, and the network has previously requested the second response from the authorization center together with the first random number and the first response as a triplet data set.